Amendments to the Drawings

Please replace the drawing sheet containing Figure 1 currently on file, with the replacement drawing sheet submitted herewith containing an amended Figure 1.

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Amendments to the Specification

The specification is amended to correct various typographical errors. In particular, paragraph [0022] is amended replacing "b, c, d and e" with "b and c"; and paragraph [0036] is amended replacing "g and h" with "g, h and i". No new matter is believed to have been added by way of these amendments.

Amendments to the Claims

Claim 1 is amended to correct typographical errors, to indicate that the executable program (formerly defined as "a program") masks the conditional jump in the cryptographic processor, and to amend the general organization of the language of the claim.

Claim 2 is amended to correct typographical errors.

Claim 4 is cancelled as the subject matter thereof was previously introduced into claim 1 in Applicant's previous response.

Claim 5 is amended in view of the cancellation of claim 4.

Claims 6-10 and 26 were withdrawn from consideration by the Examiner. Claims 6-10 and 26 are therefore cancelled without prejudice or disclaimer and Applicant reserves the right to pursue such claims in a continuing or divisional application.

Accordingly, claims 1-3 and 5 remain in the present application.

No new matter is added by way of these amendments.

Amendments to the Drawings

Figure 1 is amended to include the label "Prior Art" and a replacement sheet is submitted herewith in compliance with 37 CFR 1.121(d).

Priority

Applicant advises that certified copies of the priority applications for the present application, namely Canadian Patent Application Nos. 2,258,338; and 2,259,089 are submitted herewith.

Drawing Objections

Figure 1 was objected to for not being labeled as "PRIOR ART" (MPEP §608.02(g)). Figure 1 is amended as indicated above to overcome the Examiner's objection. The drawings are believed to now be acceptable, and indication thereof is respectfully requested.

Specification Objections

The specification is amended at page 4 (paragraph [0022]) and page 7 (paragraph [0036]) as indicated above to overcome the objections thereto.

Claim Rejections – 35 U.S.C. §112

Claims 1-5 have been rejected under 35 U.S.C. §112, second paragraph as being indefinite. The Examiner believes that it is unclear if the processor is doing the masking or if some external processor is masking the jump on the cryptographic processor.

Claim 1 is amended to better reflect the nature of the method claimed. In particular, the preamble now indicates that an executable program (formerly "a program") masks the conditional jump. The claim now also indicates that the cryptographic processor is programmed such that the executable program executes a sequence of steps. The remaining language of the claim is amended consistent with these amendments. Claim 1 is believed to now be clear and definite and explicitly point out what is claimed.

The amendments made to claim 1 are believed to address the Examiner's concern, and thus claims 1-3 and 5 are believed to comply with 35 U.S.C. §112, second paragraph.

Claim Rejections – 35 U.S.C. §101

Claims 1-5 have been rejected under 35 U.S.C. §101 for being directed to non-statutory subject matter. Applicant believes that the amendments made to claim 1 better reflect the hardware used and that a tangible output is in fact claimed. In particular, the claim recites an executable program of a cryptographic processor. Such features define the hardware and program thereof for performing the method. The claimed steps of the method include executable steps that ultimately result in particular processor instructions that mask a conditional jump to, for example, inhibit SPA and DPA attacks as exemplified in the description.

Accordingly, amended claim 1 is believed to constitute statutory subject matter and therefore comply with 35 U.S.C. §101. Claims 2-3 and 5 in their dependencies on claim 1 are also believed to comply with 35 U.S.C. §101.

Claim Rejections – 35 U.S.C. §103

Claims 1-5 have been rejected under 35 U.S.C. §103(a) as being unpatentable over applicant admitted prior art in view of Deitel et al. in C++ How to Program. Applicant respectfully traverses the Examiner's rejections as follows.

Claim 1 requires that processor instructions are inserted at a location in the conditional jump. The instructions, in part, compute a target address that is derived from the distinguishing value V and a base address constituted by a random number such that a different number of instructions are executed for each conditional jump. The Examiner believes that Figure 1 of the present application shows such a step. Applicant respectfully disagrees. In Figure 1, the steps in the "FOR" loop compare the value V against a value TH between Vmin and Vmax. This is merely a typical conditional jump and does not disclose the computation of a target address that is derived from the value V and a base address constituted by a random number such that a different number of instructions are executed for each conditional jump.

Because the address is determined from the distinguishing value and a base address constituted by a random number, rather than just a partition between the upper and lower limits Vmax and Vmin, a different number of steps is obtained. Such a target address is part of the instructions inserted into a location of the conditional jump that provides the different number of instructions as required by claim 1. Figure 1 merely shows a conditional jump itself. The instructions recited in claim 1 are inserted, and operate, in order to mask the conditional jump.

Claim 1 requires that for each evaluation of the distinguishing value against the reference value, a different number of instructions are executed for each jump. The Examiner indicates that Figure 1 (admitted prior art) does not teach this. However, the Examiner believes that page 61 of Deitel teaches such a step. Applicant respectfully disagrees. In page 61, Deitel teaches an example of a compound statement in the else part of an if/else structure. Deitel clearly does not teach the computation of a target address as recited in claim 1, such that a different number instructions are executed for each conditional jump, in fact, Deitel does not even teach in the context of a conditional jump in a processor. Therefore, Deitel clearly cannot teach a different number of instructions being executed for each conditional jump. Applicant is unsure where in page 61 the Examiner reads such a limitation, and Applicant believes that Deitel does not teach same.

Accordingly, Applicant submits that neither Figure 1 (admitted prior art) nor Deitel, alone or in combination, teach every element of claim 1. In fact Deitel does not even teach in the realm of conditional jumps in processor. Therefore, not every element of claim 1 is taught by the prior art, and there is no suggestion or motivation to modify the teachings to result in a method as recited therein.

Therefore, claim 1 is believed to clearly and patentably distinguish over the prior art cited by the Examiner, and as such is believed to be in condition for allowance. Claims 2-3 and 5 in their dependencies on claim 1 are also believed to distinguish over the art.

Summary

In view of the foregoing, Applicant respectfully submits that the present application is in condition for allowance, and action to that end is respectfully requested.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: Nov. 25 , 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL